Article Submitted to Journal of Symbolic Computation

The Parametrization of Canal Surfaces and the Decomposition of Polynomials into a Sum of Two Squares*

Günter Landsmann†, Josef Schicho‡ and Franz Winkler§

Research Institute for Symbolic Computation, Johannes Kepler University, A-4040 Linz, Austria

Abstract

A canal surface in $\mathbb{R}^3$, generated by a parametrized curve $\mathcal{C} = m(t)$, is the Zariski closure of the envelope of the set of spheres with radius $r(t)$ centered at $m(t)$. This concept is a generalization of the classical notion of an offsets of a plane curve: First, the canal surface is a surface in 3-space rather than a curve in $\mathbb{R}^2$ and second, the radius function $r(t)$ is allowed to vary with the parameter t. In case $r(t) = const$, the resulting envelope is called a pipe surface. In this paper we develop an elementary symbolic method for generating rational parametrizations of canal surfaces generated by rational curves $m(t)$ with rational radius variation $r(t)$. This method leads to the problem of decomposing a polynomial into a sum of two squares over $\mathbb{R}$. We discuss decomposition algorithms which give symbolic and numerical answers to this problem.

1. Introduction

Consider a space curve $\mathcal{C}$ parametrized by a rational map $m: \mathbb{R} \longrightarrow \mathcal{C}$ and a real-valued rational function $r(t)$. The *canal surface* with *spine curve* m and *radius variation* r is the envelope of the family of spheres centered at $m(t)$ with radius $r(t)$. Canal surfaces with constant radius function - called pipe surfaces in the literatur - have wide applications, such as shape reconstruction or robotic path planning; canal surfaces with variable radius function arise in computer aided geometric design contexts mainly as transition surfaces between pipes.

*This work has been supported by the Austrian Science Fund (FWF) under the special research area SFB F013, subprojects 03 and 04.

†guenter.landsmann@risc.uni-linz.ac.at

‡josef.schicho@risc.uni-linz.ac.at

§franz.winkler@risc.uni.linz.ac.at

There are several reasons for trying to give rational parametrizations of surfaces. One of them is the wide spread use of rational parametrizations by CAD-systems. Another one is, that points lying on the surface can be computed easily. If, furthermore, the intersection of two surfaces is to be determined, often this task can be accomplished most conveniently by representing one of the surfaces by its implicit equation while the second one is given parametrically.

Most algebraic surfaces do not admit a rational parametrization; those which do are called *unirational*.

Surprisingly canal surfaces with rational spine curve and rational radius function are unirational (Peternell Pottmann, 1997). To be precise, they admit real rational parametrizations of their real components.

It is therefore natural to ask for methods which allow one to construct a rational parametrization of a canal surface from its spine curve and radius function. The straightforward strategy would be to compute the implicit equation and to apply a general purpose parametrization algorithm (Schicho, 1998/1) or (Schicho, 1998/2), but it turns out that the defining polynomial of a canal surface is of considerably higher complexity than the original data r and m. In (Landsmann et.al., 2000) we have developed a parametrization algorithm for canal surfaces, avoiding the implicit equation and working directly with the original rational data. Our method first applies a sequence of appropriate transformations, until we arrive at a variety described by an equation in simplest possible form, rationally equivalent to the original one. Finding a rational parametrization of the latter and transforming back solves the parametrization problem for the former. In analogy to the case of plane algebraic curves, where the parametrization problem ultimately reduces to the problem of finding a "good" point on the given curve, see (Sendra Winkler, 1991),(Sendra Winkler, 1997), (Hillgarter Winkler, 1998) we have to determine a "good" curve on the surface.

As in (Peternell Pottmann, 1997) the parametrization problem is reduced to the problem of finding a representation of a rational function as a sum of two squares. This is a special case of Hilbert's 17^{th} problem (Bochnak Coste Roy, 1987; Hilbert, 1901). In (Landsmann et.al., 2000) we described a procedure for deciding this problem over $\mathbb{Q}$.

In this paper we analyze the real case, which is of particular importance in practical applications.

The new results are the following:

- a classification of all the solutions of the Two Squares Problem;
- an improved numerical algorithm for finding those solutions;
- a complexity result explaining why we cannot hope for a fast exact algorithm covering all cases.
- an improved symbolic algorithm for those cases, where an exact solution over $\mathbb{Q}$ exists.

We start in Section 2, presenting the definition of a canal surface. Section 3 describes the reduction process which eventually exposes the kernel of the parametrization problem of canal surfaces as a two squares problem. In Section 4 we discuss this problem in adequate generality and give algorithmic answers, which contain both symbolic and numerical solutions.

2. Preliminaries on Canal Surfaces

Let $m_1(t), m_2(t), m_3(t), r(t)$ be rational functions with coefficients in $\mathbb{R}$. The tuple $m = (m_1, m_2, m_3)$ defines a rational parametrization of a curve in $\mathbb{R}^3$ which will be called the *spine curve* in the sequel. Let F be the expression

$$F(x_1, x_2, x_3, t) = \sum_{i=1}^{3} (x_i - m_i(t))^2 - r(t)^2$$

and let Z denote the union of the zero sets of the denominators of m_1, m_2, m_3, r and of the numerator of r. Set $V = \mathbb{R} - Z$, $U = \mathbb{R}^3 \times V$. Then F being regular on U defines the set

$$M = \{(x_1, x_2, x_3, t) \in U \mid F(x_1, x_2, x_3, t) = 0\}$$

which is a smooth manifold of dimension 3 by the Implicit Function Theorem. Consider the projection

$$p : M \longrightarrow \mathbb{R}^3, (x_1, x_2, x_3, t) \mapsto (x_1, x_2, x_3).$$

The envelope E is the set of all critical values of p, that means

$$E = \{x \in \mathbb{R}^3 \mid \exists t\colon (x, t) \in M \text{ and } \operatorname{rank}_{(x,t)}(p) < 3\}.$$

Since p is the restriction of the linear projection $\pi\colon \mathbb{R}^4 \longrightarrow \mathbb{R}^3$, the tangent map $T_{(x,t)}(p)$ is just restriction of π to the tangent space $T_{(x,t)}(M)$ and the condition $\operatorname{rank}_{(x,t)}(p) < 3$ amounts to $\frac{\partial F}{\partial t}(x, t) = 0$. Thus the envelope is given by

$$E = \{x \in \mathbb{R}^3 \mid \exists t\colon (x, t) \in U \wedge F(x, t) = 0 \wedge \frac{\partial F}{\partial t}(x, t) = 0\}.$$

that is, the solutions in U of the system

$$\begin{aligned} \sum_{j=1}^{3} (x_j - m_j(t))^2 - r(t)^2 &= 0 \\ \sum_{j=1}^{3} (x_j - m_j(t)) \frac{dm_j(t)}{dt} + r(t)\frac{dr(t)}{dt} &= 0 \end{aligned} \tag{1}$$

after elimination of t. The associated *canal surface* $\mathcal{S}$ can now be defined as the Zariski closure of E.

3. Reduction to the Two Squares Problem

In order to find a rational parametrization of the canal surface $\mathcal{S}$ we first need a rational curve $\mathcal{C}$ on $\mathcal{S}$, which then can be used as a basis for parametrizing the whole surface by a reflection process.

A first simplification gives the substitution

$$x_j = m_j(t) + r(t)u_j \qquad (1 \leq j \leq 3). \tag{2}$$

which birationally transforms (1) to

$$\begin{aligned} \sum_{j=1}^{3} u_j^2 - 1 &= 0 \\ \sum_{j=1}^{3} \frac{dm_j}{dt} u_j + \frac{dr}{dt} &= 0. \end{aligned} \tag{3}$$

With abbreviations $a_j = \frac{dm_j}{dt}$, $(1 \leq j \leq 3)$ and $d = -\frac{dr}{dt}$, working in projective space we pass to the homogeneous system

$$\begin{aligned} u_1^2 + u_2^2 + u_3^2 - u_0^2 &= 0 \\ a_1u_1 + a_2u_2 + a_3u_3 - du_0 &= 0 \end{aligned} \tag{4}$$

which is treated as a system of equations in $\mathbb{P}^3(\mathbb{R}(t))$ and geometrically represents the intersection of a plane and a sphere. Parametrizing the linear equation we obtain the quadratic form

$$\varphi = A_1x_1^2 + A_2x_2^2 + A_3x_3^2 - 2Bx_1x_2 - 2Cx_2x_3 \tag{5}$$

with

$$A_1 = a_1^2 + a_2^2, \quad A_2 = a_2^2 + a_3^2, \quad A_3 = d^2 - a_3^2, \quad B = a_1a_3, \quad C = da_2.$$

Using the abbreviations

$$s_2 = a_1^2 + a_2^2, \; s_3 = s_2 + a_3^2$$

we first pass to the quadratic form $\psi = A_1A_3^2\varphi$, which then with the aid of the matrix

$$g = \begin{pmatrix} \frac{a_1}{s_2a_2(d^2-a_3^2)} & \frac{1}{s_2(d^2-a_3^2)} & \frac{-a_1}{a_2(d^2-a_3^2)} \\ \frac{1}{a_2a_3(d^2-a_3^2)} & 0 & \frac{-s_2}{a_2a_3(d^2-a_3^2)} \\ \frac{1}{(d-a_3)(d^2-a_3^2)a_3} & 0 & \frac{a_3d-s_3}{(d-a_3)(d^2-a_3^2)a_3} \end{pmatrix}$$

gives the equivalent quadratic form

$$\eta = g^T\psi g.$$

η expands to

$$Z_1^2 + Z_2^2 + \left(\left(\frac{dr}{dt} \right)^2 - \sum_{j=1}^{3} \left(\frac{dm_j}{dt} \right)^2 \right) \sum_{j=1}^{2} \left(\frac{dm_j}{dt} \right)^2 Z_3^2 = 0. \tag{6}$$

(see (Hillgarter, Landsmann, Schicho, Winkler, 1999) for computational details). An equation of similar shape is obtained in (Peternell Pottmann, 1997). There, the equations are derived by a geometric method.

Finding the curve $\mathcal{C}$ amounts to presenting a nontrivial solution of (6) in $\mathbb{P}^2(\mathbb{R}(t))$. Equation (6) also limits the real connected components of $\mathcal{S}$, as there are real solutions only for values of t with

$$\sum_{j=1}^{3} \left(\frac{dm_j}{dt} \right)^2 \geq \left(\frac{dr}{dt} \right)^2. \tag{7}$$

In affine coordinates

$$z_1 = \frac{Z_1}{Z_3},\ z_2 = \frac{Z_2}{Z_3}$$

a solution is found, if we are able to find a presentation of the term

$$\sum_{j=1}^{2} \left(\frac{dm_j}{dt} \right)^2 \left(\sum_{j=1}^{3} \left(\frac{dm_j}{dt} \right)^2 - \left(\frac{dr}{dt} \right)^2 \right)$$

as a sum of two squares. Using Fibonacci's formula

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 \tag{8}$$

it is enough to decompose

$$\sum_{j=1}^{3} \left(\frac{dm_j}{dt} \right)^2 - \left(\frac{dr}{dt} \right)^2.$$

Clearing denominators produces an expression of equal type. As, in practice, the input data will have rational coefficients, we are faced with the following problem:

Problem 1: *[Two Squares Problem] Given a polynomial $f \in \mathbb{Q}[t]$, find a decomposition $f = g^2 + h^2$ with $g, h \in \mathbb{R}[t]$.*

Of course, f has to be globally positive. But this condition is also sufficient for decomposition. We present here the general result, formulated for rational functions.

Lemma 3.1: *Let ρ be a rational function in $\mathbb{R}(t)$. Then ρ is a sum of two squares in $\mathbb{R}(t)$ if and only if $\rho = \frac{F}{G}$ with $F, G \in \mathbb{R}[t]$ and $FG \geq 0$.*

A proof can be found in (Landsmann et.al., 2000). We postpone the treatment of Problem 1 to Section 4.

Once a solution $(z_1 : z_2 : z_3)$ of (6) is at hand, application of the inverse transformations yields a curve $\mathcal{C}$ on the surface $\mathcal{S}$ and we construct a rational parametrization of $\mathcal{S}$ by simply rotating $\mathcal{C}$ around the spine curve m. The details of this construction may be found in (Peternell Pottmann, 1997) or (Landsmann et.al., 2000).

The above considerations lead also to the following conclusion:

THEOREM 3.1: *The canal surface given by the spine curve $m = (m_1(t), m_2(t), m_3(t))$ and the radius function $r(t)$, with $m_1(t), m_2(t), m_3(t), r(t) \in \mathbb{R}(t)$, admits a rational parametrization over the reals in accordance with the spine* [¶] *if and only if $\left(\frac{dm_1}{dt}(x)\right)^2 + \left(\frac{dm_2}{dt}(x)\right)^2 + \left(\frac{dm_3}{dt}(x)\right)^2 \geq \left(\frac{dr}{dt}(x)\right)^2$ for almost all $x \in \mathbb{R}$.*

In general the rational function $\rho := \left(\frac{dm_1}{dt}\right)^2 + \left(\frac{dm_2}{dt}\right)^2 + \left(\frac{dm_3}{dt}\right)^2 - \left(\frac{dr}{dt}\right)^2$ need not be positive. In this case we have to restrict to intervals on which $\rho \geq 0$ and to reparametrize the spine curve. In the new setting the condition $\rho \geq 0$ is then valid on the whole real axis. If e.g. ρ is positive on $[a, b] \subset \mathbb{R}$, we can apply the reparametrization $t = \frac{b\theta^2+a}{\theta^2+1}$. In case $\rho \geq 0$ on $[a, \infty)$ we can use $t = \theta^2 + a$. Obviously, then, each point of the curve component under consideration is passed twice, so a proper parametrization cannot be achieved. This problem can be resolved by restricting the parameters to positive values.

The pseudo-code of a parametrization algorithm for canal surfaces is now given by the following steps:

Algorithm CANAL_SURFACE

Input: $m_1(t), m_2(t), m_3(t), r(t)$ rational functions determining a canal surface $\mathcal{S}$;
Output: $X_1(t, \eta), X_2(t, \eta), X_3(t, \eta)$ rational parametrization of a component of $\mathcal{S}$;

1. compute $\rho(t) = \sum_{j=1}^{3} \dot{m}_j(t)^2 - \dot{r}(t)^2$;
2. choose an interval (a, b) on which $\rho \geq 0$;
3. if $(a, b) \neq \mathbb{R}$ then reparametrize $t := t(\theta)$, so that $\rho(\theta) \geq 0$;
4. compute a decomposition $\rho = \sigma^2 + \tau^2$;
5. use identity (8) to obtain a solution of (6);
6. apply the inverse transformations to get a curve $\mathcal{C}$ on the canalsurface $\mathcal{S}$;
7. compute a surface parametrization of $\mathcal{S}$ by rotating $\mathcal{C}$ around the spine.

EXAMPLE 1: [Viviani's Temple with variable radius] This space curve is defined as the intersection of a sphere of radius $2a$ and a circular cylinder of radius a:

$$x^2 + y^2 + z^2 = 4a^2$$

[¶]This means that one parameter of the surface parametrization equals the curve parameter.

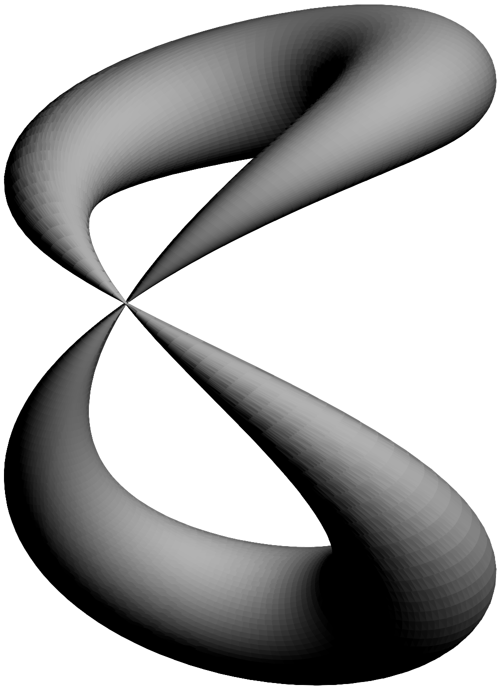

Figure 1: canal surface around Viviani's temple

$$(x-a)^2 + y^2 \;=\; a^2$$

Its rational parametrization can be given by

$$m(t) = \left(\frac{2a(1-t^2)^2}{(1+t^2)^2}, \frac{4at(1-t^2)}{(1+t^2)^2}, \frac{4at}{1+t^2} \right).$$

We set $a = 1$ and compute a parametrization of the canal surface with spine m and radius $r(t) = \frac{t}{1+t^2}$. It turns out that the term

$$\dot{m}_1^2 + \dot{m}_2^2 + \dot{m}_3^2 - \dot{r}^2 = \frac{31t^4 + 2t^2 + 31}{(1+t^2)^4},$$

thus, it can be written as

$$\left(\frac{(t^2 + \frac{1}{31})\sqrt{31}}{(t^2+1)^2} \right)^2 + \left(\frac{8\sqrt{465}}{31(t^2+1)^2} \right)^2.$$

The coefficients of this decomposition are in $\mathbb{Q}[\sqrt{31}, \sqrt{465}]$ which is of degree 4 over $\mathbb{Q}$. From this we can compute a rational parametrization of the canal surface drawn in Figure 1 by applying steps 5-8 (cf. Landsmann et.al. (2000))

Note that it is possible to recover a representation of ρ as a sum of two squares from a paramerization obtained by whichever method. Therefore the computational complexity of Canal surface parametrization equals that of the Two Squares Problem.

4. The Decomposition into a Sum of Squares

The crucial point in the algorithm **CANAL_SURFACE** is the discovery of σ, τ such that $\sigma^2 + \tau^2 = \rho$ in Step 4. By Lemma 3.1 we may assume that $\rho = \frac{F}{G}$ with $F, G \in \mathbb{R}[t]$ and $F \geq 0$ and $G \geq 0$. Obviously this problem can be solved if we are able to find a decomposition $f = g^2 + h^2$ for polynomials $f \in \mathbb{R}[t]$ with $f \geq 0$ into a sum of two squares of polynomials $g, h \in \mathbb{R}[t]$. In view of Identity (8) we propose the following concept:

Algorithm NUMERIC_DECOMPOSITION1

Input: $f \in \mathbb{R}[t]$ positive;
Output: $g, h \in \mathbb{R}[t]$ with $g^2 + h^2 = f$;

1. compute a factorization of f into quadratic polynomials:
   $f = Q_1^{d_1} \cdots Q_r^{d_r}$;
2. for each j with $1 \leq j \leq r$
   write the quadratic factor $Q_j = a_j t^2 + b_j t + c_j$ as
   $$Q_j = \left(\sqrt{a_j}t + \frac{b_j}{2\sqrt{a_j}}\right)^2 + \sqrt{c_j - \frac{b_j^2}{4a_j}}^{\,2};$$
3. combine the above polynomials according to formula (8).

The individual concepts make sense because f is assumed to be positive. The critical point in this algorithm is the fact that it requires factorization of univariate polynomials into linear and quadratic irreducible factors. This is no problem numerically, but it is fairly difficult to do symbolic factorization for a generic polynomial in $\mathbb{Q}[t]$. It is therefore desirable to find a solution of the equation in Step 4 within the rationals.

4.1. The Decomposition Problem

Before constructing an algorithm which searches for rational solutions of particular Two Squares Problems, we make some general observations with respect to the structure of Two Squares decompositions. Since there are several completely different decompositions of positive polynomials in $\mathbb{R}[t]$, we try to obtain an exhausting classification.

Example 2: Consider the decomposition

$$F = t^6 - 2t^5 + 6t^4 - 14t^3 + 19t^2 - 14t + 5 = (t^3 - t^2 + 2t - 2)^2 + (t^2 - 3t + 1)^2.$$

The polynomials

$$u = \frac{1}{3}t^3 + \left(-\frac{2}{3}\sqrt{2} - \frac{1}{3}\right)t^2 + \left(2\sqrt{2} + \frac{2}{3}\right)t - \frac{2}{3}\sqrt{2} - \frac{2}{3}$$

$$v = \frac{2}{3}\sqrt{2}t^3 + \left(\frac{1}{3} - \frac{2}{3}\sqrt{2}\right)t^2 + \left(-1 + \frac{4}{3}\sqrt{2}\right)t + \frac{1}{3} - \frac{4}{3}\sqrt{2}$$

yield another decomposition $F = u^2 + v^2$.

For a polynomial p with complex coefficients, $\bar{p}$ denotes the complex conjugate of p, i.e., if $p = \sum_k p_k t^k$, then $\bar{p} = \sum_k \bar{p_k} t^k$. Consider the maps

$$\begin{aligned} \mathbf{s}\colon \mathbb{R}[t] \times \mathbb{R}[t] &\longrightarrow \mathbb{R}[t], \quad (g,h) \mapsto g^2 + h^2 \\ \mathbf{c}\colon \mathbb{R}[t] \times \mathbb{R}[t] &\longrightarrow \mathbb{C}[t], \quad (g,h) \mapsto g + ih \end{aligned}$$

and the norm

$$\mathbf{N}\colon \mathbb{C}[t] \longrightarrow \mathbb{R}[t], \ p \mapsto p\bar{p}.$$

For $f \in \mathbb{R}[t]$ let $D_{\mathbb{R}}(f)$ denote the set of all possible decompositions, i.e.,

$$D_{\mathbb{R}}(f) = \{(g,h) \in \mathbb{R}[t] \times \mathbb{R}[t] \mid g^2 + h^2 = f\}.$$

The $\mathbb{R}-$linear isomorphism $\mathbf{c}$ maps $D_{\mathbb{R}}(f)$ onto the set

$$D_{\mathbb{C}}(f) = \{p \in \mathbb{C}[t] \mid p\bar{p} = f\}.$$

This has two consequences. First, with the aid of the map $\mathbf{c}$, we realize, that any decomposition of a polynomial $f \in \mathbb{R}[t]$ into a sum of two squares in $\mathbb{R}[t]$ is in fact some special kind of factorization in $\mathbb{C}[t]$. Second, the map $\mathbf{c}$ allows to transport the action of the circle group to the real situation, so that we can pass to orbits. Since two decompositions $f = g^2 + h^2$ and $f = h^2 + g^2$ are essentially the same, we identify them by an appropriate group action:

Let $\mathbb{S}^1 \subset \mathbb{C}$ denote the one-dimensional torus, and $S_2 = \{1, \tau\}$ the 2-element group, written multiplicatively. Both groups act on $\mathbb{C}[t]$, the torus by scalar multiplication, and S_2 by the stipulation

$$\tau \cdot P = \bar{P}.$$

Hence there is a group action of the free product $\mathbb{S}^1 \star S_2$ on $\mathbb{C}[t]$. The map $\mathbf{c}$ transports the orbits in $\mathbb{C}[t]$ to $\mathbb{R}[t] \times \mathbb{R}[t]$. We write $(g_1, h_1) \sim (g_2, h_2)$ if the two pairs belong to the same orbit.

LEMMA 4.1: *Take $g_1, h_1, g_2, h_2 \in \mathbb{R}[t]$ and let $p_1 = \mathbf{c}(g_1, h_1)$ and $p_2 = \mathbf{c}(g_2, h_2)$. Then*

$$(g_1, h_1) \sim (g_2, h_2) \ \Leftrightarrow \ \exists \lambda \in \mathbb{S}^1 \, (p_2 = \lambda p_1 \vee p_2 = \lambda \bar{p}_1)$$

Proof: Elements $x \in \mathbb{S}^1 \star S_2$ are finite products of the form

$$x = \lambda_1 \tau \lambda_2 \tau \cdots \ \text{or} \ x = \tau \lambda_1 \tau \lambda_2 \cdots$$

where $\lambda_j \in \mathbb{S}^1$. In both cases the action of x on an element $p \in \mathbb{C}[t]$ produces either a polynomial μp or $\mu \bar{p}$, with $\mu \in \mathbb{S}^1$. The first variant arises exactly in the case where the number of occurences of τ in x is even.[‖] □

[‖]The groups $\mathbb{S}^1$ and S_2 considered as subgroups of $\mathrm{Aut}_{\mathbb{Z}}\mathbb{C}[t]$ commute, whence their complex product is the group which effectively acts on $\mathbb{C}[t]$.

Corollary 1: *Let f, g, h be in $\mathbb{R}[t]$ and assume that $f = g^2 + h^2$. Then the orbit of (g, h) is contained in $D_{\mathbb{R}}(f)$.*

Proof: Take g_1, h_1, g_2, h_2 in $\mathbb{R}[t]$ with $(g_1, h_1) \sim (g_2, h_2)$, and let p_1, p_2 denote $\mathbf{c}(g_1, h_1), \mathbf{c}(g_2, h_2)$ respectively. There is a $\lambda \in \mathbb{S}^1$ with $p_2 = \lambda p_1 \vee p_2 = \lambda \bar{p}_1$. Therefore, in both cases, $\mathbf{N}(p_1) = \mathbf{N}(p_2)$, i.e., $\mathbf{s}(g_1, h_1) = \mathbf{s}(g_2, h_2)$. $\square$

The two decompositions in Example 2 are eqivalent. The second one is derived from the first by multiplying with $\lambda = \frac{1}{3} + \frac{2\sqrt{2}}{3}i$.

Theorem 4.1: *Let $f \in \mathbb{R}[t]$ be a positive squarefree polynomial of degree $2n > 0$. There are then exactly 2^{n-1} pairwise inequivalent decompositions $f = g^2 + h^2$.*

Proof: First assume f to be monic. From the factorization of f in $\mathbb{C}[t]$

$$f = \prod_{j=1}^{n} ((t - \alpha_j)(t - \bar{\alpha_j}))$$

with $\alpha_j \neq \alpha_k$ for $j \neq k$, one realizes that there are 2^n separations of f into $f = P\bar{P}$, coming from distinct collections of the linear factors. Taking into account that conjugate polynomials get identified, there are 2^{n-1} left.

Now, equivalent decompositions of f produce complex factors, which either are associated, or one is associated to the conjugate of the other; hence distinct separations are inequivalent. Obviously every decomposition is equivalent to one such separation, hence the set $D_{\mathbb{R}}(f)$ consists of exactly 2^{n-1} orbits.

In the general case, write $f = a\hat{f}$ with $\hat{f}$ monic and $a > 0$. Then $D_{\mathbb{C}}(f) = \sqrt{a} D_{\mathbb{C}}(\hat{f})$ proves the assertion. $\square$

So far, our considerations lead to the following improvement of Algorithm $NUMERIC\_DECOMPOSITION1$:

Algorithm NUMERIC_DECOMPOSITION2

Input: $f \in \mathbb{R}[t]$ positive;
Output: $g, h \in \mathbb{R}[t]$ with $g^2 + h^2 = f$;

1. factor f into squarefree parts F_j;
2. for each j
   (a) factor F_j over $\mathbb{C}$;
   (b) choose a separation p_j with $p_j \bar{p}_j = F_j$;
   (c) set $g_j := \mathrm{Re}(p)$, $h_j := \mathrm{Im}(p)$;
3. combine the pairs (g_j, h_j) according to formula (8).

The next theorem gives a flair of the complexity of an arbitrary symbolic decomposition algorithm. Note that a randomly chosen rational polynomial usually has the maximal possible Galois group**.

THEOREM 4.2: *Let $f \in \mathbb{Q}[t]$ be a positive irreducible polynomial of degree $2n$ over $\mathbb{Q}$. Decompose f into $f = g^2 + h^2$ $(g, h \in \mathbb{R}[t])$. If the Galois group of f is the symmetric group S_{2n}, then the coefficients of g, h involve algebraic numbers of degree at least $\frac{1}{2}\binom{2n}{n}$.*

Proof: Set $p = g + ih \in \mathbb{C}[t]$, then $f = p\bar{p}$ and $\deg p = n$. Let

$$p = \beta(t - \alpha_1) \cdots (t - \alpha_n)$$

be the complete factorization of p; thus $\bar{p} = \bar{\beta}(t - \bar{\alpha_1}) \cdots (t - \bar{\alpha_n})$ and $\beta\bar{\beta} = f_{2n}$. Set $p_1 = \frac{1}{\beta}p$. We introduce the notations $E = \mathbb{Q}(\alpha_1, \ldots, \alpha_n),\ F = \mathbb{Q}(\alpha_1, \ldots, \alpha_n, \bar{\alpha_1}, \ldots, \bar{\alpha_n})$, $G = \mathrm{Gal}\, f = \mathrm{Aut}_{\mathbb{Q}} F$ and $A = \{\alpha_1, \ldots, \alpha_n\}$. Furthermore let C denote the smallest field containing the coefficients of p, and, analogous, C_1 for p_1. Finally let K be the smallest field containing the coefficients of g and h.

Obviously, F is the splitting field of f over $\mathbb{Q}$, and E the splitting field of p_1 over C_1. Complex conjugation yields an isomorphism from E with $\bar{E} = \mathbb{Q}(\bar{\alpha_1}, \ldots, \bar{\alpha_n})$. The group G is isomorphic to a transitive subgroup of $S_{A \cup \bar{A}} \cong S_{2n}$ of order at least $2n$.

Now, the coefficients of p_1 being elementary symmetric polynomials in $\alpha_1, \ldots, \alpha_n$ are expressible as polynomials involving the elementary symmetric polynomials in all variables of $A \cup \bar{A}$, and $\bar{\alpha}_1, \ldots, \bar{\alpha}_n$. This implies $C_1 \subseteq E \cap \bar{E}$.

Since the elements of $\mathrm{Gal}(F/E)$ commute with those of $\mathrm{Gal}(F/\bar{E})$ we conclude

$$\mathrm{Gal}(F/(E \cap \bar{E})) = \mathrm{Gal}(F/E)\mathrm{Gal}(F/\bar{E}) \cong \mathrm{Gal}(F/E) \times \mathrm{Gal}(F/\bar{E}).$$

With the abbreviations $e = |\mathrm{Gal}(F/E)|,\ d = [E \cap \bar{E} \colon C_1]$ we obtain

$$[F \colon E \cap \bar{E}] = |\mathrm{Gal}(F/(E \cap \bar{E}))| = |\mathrm{Gal}(F/E)||\mathrm{Gal}(F/\bar{E})| = e^2,$$

hence $[E \colon E \cap \bar{E}] = e$ and therefore

$$e^2 d \cdot [C_1 \colon \mathbb{Q}] = |G| \text{ and } ed \leq n! \tag{9}$$

Now assume that $G \cong S_{2n}$. Then any permutation of the set $\bar{A}$ extends to an automorphism in $\mathrm{Gal}(F/E)$, whence $\mathrm{Gal}(F/E) \cong S_n$ and $e = n!$. Condition (9) gives now

$$(n!)^2 d \cdot [C_1 \colon \mathbb{Q}] = (2n)! \text{ and } d = 1,$$

therefore

$$[C_1 \colon \mathbb{Q}] = \frac{(2n)!}{(n!)^2} = \binom{2n}{n}.$$

**We denote the symmetric group on n letters by S_n.

Immediately from the definitions one derives $C_1(\beta) = C \subseteq K(i)$. Since $K \subseteq \mathbb{R}$, $[K(i): K] = 2$ is evident. Hence

$$[K(i): C][C: C_1][C_1: \mathbb{Q}] = 2[K: \mathbb{Q}] \text{ and so}$$

$$[K: \mathbb{Q}] = \frac{1}{2}[K(i): C][C: C_1][C_1: \mathbb{Q}] \geq \frac{1}{2}\binom{2n}{n}.$$

□

Remark 1: The result states that, for a randomly chosen positive polynomial, any solution of the Two Squares Problem lies in a field extension of exponentially high degree. It is clear that every exact algorithm must in particular compute the extension containing the coefficients of the solution. Therefore we cannot expect an exact algorithm producing a solution for every case in reasonable time.

Remark 2: As multiplication of particular solutions of a Two Squares Problem with arbitrary complex numbers of modulus 1 produces new solutions, the coefficients of the participating polynomials can be algebraic numbers of arbitrary high degree, or even transcendental numbers.

Example 3: The polynomials

$$\phi = \frac{1}{5}\pi t^3 + \left(\frac{-1}{5}\pi - \frac{1}{5}\sqrt{25-\pi^2}\right)t^2 + \left(\frac{2}{5}\pi + \frac{3}{5}\sqrt{25-\pi^2}\right)t - \frac{2}{5}\pi - \frac{1}{5}\sqrt{25-\pi^2}$$

$$\psi = \frac{1}{5}\sqrt{25-\pi^2}t^3 + \left(\frac{-1}{5}\sqrt{25-\pi^2} + \frac{1}{5}\pi\right)t^2 + \left(\frac{2}{5}\sqrt{25-\pi^2} - \frac{3}{5}\pi\right)t - \frac{2}{5}\sqrt{25-\pi^2} + \frac{1}{5}\pi$$

yield yet another decomposition of

$$t^6 - 2t^5 + 6t^4 - 14t^3 + 19t^2 - 14t + 5$$

which now contains transcendental coefficients.

4.2. Solutions over $\mathbb{Q}$

Even though we cannot expect small exact solutions of the Two Squares Problem in general, there are instances for which exact solutions in $\mathbb{Q}$ do exist. In the last decade algorithms have been developed, which, applied to this special situation, produce solutions, if they exist; we can e.g. consider the Two Squares Problem as a specific functional decomposition problem $f(t) = (x^2 + y^2) \circ (g(t), h(t))$ so we might apply a functional decomposition algorithm to the polynomial f and then search through the list of decomposition factors. If $x^2 + y^2$ appears in this list, we have an affirmative answer to the Two squares Problem.

In (Landsmann et.al., 2000) we gave an algorithm, which is tailored to the specific problem of two squares. Here we present an improvement of this algorithm both in terms of simplicity and in terms of computational complexity. As in (Landsmann et.al., 2000), the method works for an arbitrary computable field k of characteristic $\neq 2$, provided that k admits computable factorization and allows solution of the Two Squares Problem for constants. If k is the field of rationals, then, for decision of the last task, we can use Fermat's Theorem: c is a sum of two squares if and only if every prime occuring with an odd exponent in the numerator or in the denominator is congruent 1 modulo 4. In the affirmative case, a representation can be found easily.

In the following we always assume that -1 is not a square in k. Also, we adhere to the convention that *gcd*'s be monic.

LEMMA 4.2: *Let F be an irreducible monic polynomial in $k[t]$. If F is a factor of a sum of two squares of polynomials in $k[t]$ which are not both multiples of F, then F itself is a sum of two squares.*

Proof: $FG = P^2+Q^2$, $\gcd(P,Q) = 1$. In $k(i)[t]$ we have $FG = (P+iQ)(P-iQ)$. If F and $P+iQ$ were coprime then $F|P-iQ$ and so $F|P+iQ$ which is a contradiction. Hence both of $\gcd(F, P+iQ)$ and $\gcd(F, P-iQ)$ are nonconstant. Applying conjugation, one realizes that $\gcd(F, P-iQ)$ is the conjugate of $\gcd(F, P+iQ)$. A common factor of these two polynomials would divide P and Q thence $\gcd(F, P-iQ)$ and $\gcd(F, P+iQ)$ are coprime. Writing $\gcd(F, P+iQ) = U+iV$ one concludes that

$$U^2 + V^2 = (U+iV)(U-iV)|F.$$

Hence F is associated to U^2+V^2. Now, since gcs's having leading coefficient 1, we see that U^2+V^2 is monic, therefore $F = U^2+V^2$. □

The following lemma reduces the Two Squares Problem to the case of irreducible polynomias.

LEMMA 4.3: *A polynomial $F \neq 0$ is a sum of two squares if and only if its leading coefficient is a sum of two squares and all its monic irreducible factors are sums of two squares.*

Proof: Suppose $F = P^2+Q^2$. We may write P as at^m plus terms of lower degree, and Q as bt^n plus terms of lower degree. Assume $m \geq n$ without loss of generality. Because -1 is not a square, there is no cancellation in degree $2m$ in the sum P^2+Q^2. Therefore $\deg(F) = 2m$ and $\mathrm{lcoeff}(F) = a^2+b^2$ if $m = n$, and $\mathrm{lcoeff}(F) = a^2$ if $m > n$. The second condition follows immediately from lemma 4.2.

Conversely, suppose we have written the monic irreducible factors of F as sums of two squares. Applying Fibonacci's formula we obtain a representation of the monic polynomial F' associated to F as a sum of two squares. By assumption, the leading coefficient c of F is a sum of two squares. Then another application of Fibonacci's formula represents $F = cF'$ as a sum of two squares. □

Finally, here is the solution for the irreducible case.

LEMMA 4.4: *Let F be an irreducible polynomial in $k[t]$. Then F is associated to a sum of two squares if and only if -1 is a square in the field extension $k' := k[t]/\langle F \rangle$.*

Proof: Suppose that $P^2 + Q^2 = cF$. Then Q is not divisible by F, hence Q is invertible in k' and $-1 = (P \cdot Q^{-1})^2$ in k'.

Conversely, suppose that -1 is a square in k', and let R be a polynomial such that $R^2 + 1$ is zero modulo F. Then we get $R^2 + 1 = FG$ for some G. By Lemma 4.2, F is associated to a sum of two squares. □

REMARK 3: If -1 is a square, then

$$F = \left(\frac{F+1}{2}\right)^2 + \left(\frac{F-1}{2\sqrt{-1}}\right)^2,$$

hence any polynomial can be easily written as a sum of two squares.

Algorithmically, the problem of deciding whether -1 is a square in k' is a special case of polynomial factorization (-1 is a square if and only if $x^2 + 1$ is reducible in $k'[x]$). For this subproblem, we refer to (Landau, 1985; Lenstra, 1982; Wang, 1976).

The given proof for the existence criterion is constructive, in the sense that it allows to construct a representation of F as a sum of two squares in case the criterion is fulfilled. The following algorithm is extracted from this proof.

Algorithm TWO_SQUARES

Input: F polynomial;
Output: (X, Y) polynomials such that $X^2 + Y^2 = F$;

1. compute the factorization $F = c \prod_j P_j^{e_j}$ into monic irreducible polynomials;
2. decide if $c = \text{lcoeff(F)}$ is a sum of two squares;
3. if 2. = `FALSE` then RETURN(`NotExist`) and exit; else choose two constants (X, Y) such that $X^2 + Y^2 = c$;
4. for each j
   if e_j is even then $(X, Y) = (P_j^{e_j/2} X, P_j^{e_j/2} Y)$;
   else
   (a) $k' := k[t]/\langle P_j \rangle$;
   (b) if $x^2 + 1$ is irreducible over k' then RETURN(`NotExist`) and exit;
   else
      i. $R(t) :=$ a polynomial such that $R^2 + 1 = 0$ in k';

ii. $U + iV := \gcd(R + i, P_j)$ in $k(i)[t]$;

iii. $(X, Y) := (XU + YV, XV - YU)$;
RETURN (X, Y).

EXAMPLE 4: We want to represent the polynomial

$$F = t^6 - 2t^5 + 6t^4 - 14t^3 + 19t^2 - 14t + 5$$

as a sum of two squares. The polynomial is irreducible over $\mathbb{Q}$. The leading coefficient is 1, so the first condition is fulfilled. Next, we have to check whether -1 is a square modulo F. It turns out, e.g. by a call of Maple, that $-1 = R^2$ in $\mathbb{Q}[t]/\langle F \rangle$, where

$$R = \frac{7}{19}t^5 - \frac{10}{19}t^4 + \frac{39}{19}t^3 - \frac{73}{19}t^2 + \frac{94}{19}t - \frac{47}{19}$$

So now we know that a solution exists.

Next we compute

$$\gcd(R + \sqrt{-1}, F) = t^3 - t^2 + 2t - 2 + I(-t^2 + 3t - 1).$$

Hence we obtain the representation

$$F = (t^3 - t^2 + 2t - 2)^2 + (-t^2 + 3t - 1)^2.$$

5. Conclusion

We have discussed the problem of finding real rational parametrizations of canal surfaces whose spine curve and radius variation are given by rational functions. We have stressed a purely symbolic approach which resulted in finding a decomposition of a univariate real polynomial as a sum of two squares, so this problem is surveyed in adequate generality. Our complexity result states that finding such a decomposition is in fact partial factorization of the polynomial under consideration. In case this can be done over $\mathbb{Q}$ we gave an algorithm for performing this task.

For polynomials with rational coefficients it remains an open problem to do exact decomposition without factorization if solutions can only be found in algebraic extensions of $\mathbb{Q}$.

References

J. Bochnak, M. Coste, M.-F. Roy, *Géometrie Algébrique Réelle*, Springer, (1987).

D. Hilbert, (1901). Mathematische Probleme, *Archiv für Mathematik und Physik*, **1**, 44–63. 213–237.

E. Hillgarter, G. Landsmann, J. Schicho, F. Winkler, Generalized offsets as envelopes of a one-parameter set of spheres, *Tech. Rep. 99-20, RISC-Linz, Univ. Linz, A-4040 Linz*, (1999).

E. Hillgarter, F. Winkler, Points on algebraic curves and the parametrization problem, *Automated Deduction in Geometry*, D. Wang,L. Fariñas H. Shi, (1997). Springer, 185–203.

S. Landau, (1985). Factoring polynomials over algebraic number fields, *SIAM Journal on Computing 14*, **1**, 184–195.

G. Landsmann, J. Schicho, F. Winkler, E. Hillgarter, Symbolic parametrization of pipe and canal surfaces, *ISSAC-2000*, 194–200. C Traverso, ACM Press, (2000).

A. K. Lenstra, Factoring polynomials over algebraic number fields, *Tech. rep., Stichting Mathematisch Centrum, Kruislaan 413 1098 SJ Amsterdam*, (1982).

M. Peternell, H. Pottmann, (1997). Computing rational parametrizations of canal surfaces, *Journal of Symbolic Computation*, **23**, 255–266.

J. Schicho, Rational parameterization of real algebraic surfaces, *ISSAC-98*, (1998). ACM Press, 302–308.

J. Schicho, (1998). Rational parametrization of surfaces, *Journal of Symbolic Computation*, **26**, 1–30.

J. Sendra, F. Winkler, (1991). Symbolic parametrization of curves, *Journal of Symbolic Computation 12*, **6**, 607–632.

J. Sendra, F. Winkler, (1997). Parametrization of algebraic curves over optimal field extensions, *Journal of Symbolic Computation*, **23, 2/3**, 191–208.

P. S. Wang, (1976). Factoring multivariate polynomials over algebraic number fields, *Math. Comp. 32*, **144**, 324–336.